Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Transition Process for 700 MHz Public Safety Broadband Waiver Recipients	))	PS Docket No. 12-94
	)	
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)))	PS Docket No. 06-229

To: Chief, Public Safety and Homeland Security Bureau

COMMENTS OF CITY OF CHESAPEAKE, VIRGINIA DALLAS/FORT WORTH INTERNATIONAL AIRPORT

The City of Chesapeake, Virginia ("Chesapeake") and the Dallas/Fort Worth International Airport ("DFW"), through counsel and pursuant to Section 1.415 of the Commission's Rules, 47 C.F.R. §1.415, hereby respectfully submits their comments in response to the *Public Notice* in the above-captioned proceeding.[1]

[1] *Public Safety and Homeland Security Bureau Seeks Comment On Transition Process For 700 MHz Public Safety Broadband Waiver Recipients*, DA 12-555 (released April 6, 2012).

I. BACKGROUND

A. The City Of Chesapeake, Virginia

Although Chesapeake and DFW have previously filed comments in this proceeding, it is perhaps important to reiterate each entity's interest in this proceeding. For its part, the City of Chesapeake, Virginia is one of the jurisdictions which received an early-build Waiver from the Commission. Access to the 700 MHz public safety broadband spectrum will enable Chesapeake to deploy a local wireless data network that will facilitate high-speed mobile data IP connectivity to the City's established network, thereby serving the interests of public safety and public service responders.

Currently, the City is forced to rely too heavily on its public safety voice radio network. While the Chesapeake Police Department obtains service from a commercial broadband wireless data network, that network lacks sufficient RF coverage to provide network connectivity to emergency responders in all but the most populated areas of the City. In areas not served by the commercial wireless network, on-scene responders must transmit and obtain vital information via the current voice radio network, thus limiting the amount of data that an Incident Commander can obtain for making split-second decisions to preserve life and property during an emergency event. In addition, the reliability of this commercial wireless network is questionable during and after weather events that may cause damage to the commercial wireless system and render it inoperable. Finally, the subscription costs for access to the current commercial wireless network do not provide a return to the City beyond the ability to remotely connect to the City's private network.

The Chesapeake Fire Department, for example, does not operate on any broadband wireless data network. Therefore, on-scene responders are required to obtain vital information via the current voice radio network regardless of their location, similarly limiting the ability of Incident Commanders to preserve life and property during emergencies.

In addition, Public Service responders, which are heavily utilized during emergency operation activation periods, such as hurricane strikes, have no method for remote wireless connectivity to the City's private network to provide damage assessment and recovery reporting. All Public Service reporting during emergency operations activation periods must be accomplished via the City's current voice radio network.

Though a regional unlicensed mobile data network has been deployed on spectrum in the 900 MHz band through the COPS program in 2004, this spectrum does not provide the operational coverage required for public safety emergency responders and has been plagued by connectivity issues with client devices during numerous system tests in the Hampton Roads region. To obtain adequate RF coverage, at least 300 new access points would have to be deployed in the City. The cost of such a deployment is prohibitive. Use of the 700 MHz public safety broadband spectrum would allow the City to achieve its communications goals at a lesser expense.

Since the grant of the Waiver, and after the loss of a BTOP grant to fund the system's construction, the City has actively sought alternative methodologies to enable immediate system construction. In addition, the Chesapeake has actively participated in various committees which are working to ensure that the nationwide 700 MHz network is built, and that the network is truly interoperable. As part of that effort, Chesapeake has met with vendors to develop methodologies by which Chesapeake can leverage its upgrade to its 800 MHz land mobile radio system, in order to implement its 700 MHz broadband system at the same time. In pursuit of that outcome, Chesapeake has retained technical expertise, and was poised to release a Request for Proposals when the bill creating FirstNet became law and questions were raised as to whether Waiver Recipients could proceed with their build-outs.

B. Dallas/Fort Worth International Airport

Located halfway between the cities of Dallas and Fort Worth, Texas, the Dallas/Fort Worth International Airport is the world's third busiest, offering nearly 1,750 flights per day and serving 60 million passengers a year. DFW provides non-stop service to 144 domestic and 44 international destinations worldwide. Sitting on a campus of 18,000 acres, the airport is larger than the island of Manhattan. The Airport operates 5 passenger terminals, two full service hotels and is an international port of entry to the Unites States. For the past four years in a row, DFW has ranked in the top five for customer service among large airports worldwide in surveys conducted by Airports Council International.

DFW International Airport is an incorporated city and a sovereign jurisdiction within the State of Texas. The Airport has a commissioned police department that includes 179 sworn police officers, a fire department consisting of 195 commissioned firemen, and a private security detail of 115 security officers.

DFW maintains a Critical Communications Infrastructure to provide RF communications to all divisions of the Airport. The Airport's system was installed initially with 5-channels to support analog transmissions. The system was upgraded to 10-channels in 1995. The Radio System was upgraded to full digital ProVoice communications in November of 2001 and its communications were digitally encrypted for greater security in September of 2002.

Today, the Airport's RF communications environment consists of numerous Radio System platforms, in-building distributed antenna systems, distributed bi-directional amplifier deployments, conventional and trunked technologies. The current environment contains 800 MHz trunking, 700 MHz trunked, 450 MHz UHF conventional, 150 MHz VHF conventional, fully digital and analog transmissions capabilities and complete digital security encryption both at the radio level and the system level. The Critical Communications Infrastructure is supported by a fully fault tolerant redundant network switching center with two fully installed sites located in disparate locations. The center supports circuit switching CDMA technology from the Airport's legacy communications environment, advanced Packet switching TDMA, technology from recent system deployments, and fully compliance APCO P25 communications protocols through inner subsystem interfaced to radio systems of all major manufacturers. The Critical Communications Infrastructure is a Harris Communications Private Radio System.

DFW Airport is probably the most prominent terrorist target in the Northeastern region of the State of Texas as well as the region's largest economic generator. From a security perspective, the Airport relies heavily on technology to enables it to detect and apprehend persons that pose potential threats to the Airport. A very important need is the ability to transfer video from the Airports security surveillance environment to security officials within the passenger terminals and to police vehicles on the DFW Campus. The ability for DFW to transmit high speed data for similar reasons is also critical to the successful operations of the Airport. Decisions made regarding the use of 700 MHz broadband spectrum from the public safety trust are very important to the Airport as they affect its ability to provide a safe and secure environment for its employees, its tenants and to the traveling public.

On December 13, 2011, DFW submitted an application to construct a 700 MHz public safety broadband system with the State of Texas, one of the Waiver Recipients.[2] The proposed system, entirely self-funded by DFW, has been on hold since that time, as Texas works with the Commission to demonstrate its interoperability with the rest of the nationwide network.

II. COMMENTS

Initially, it should be noted that Chesapeake participated in the review of the Comments submitted by the Operators Advisory Committee to the Public Safety Spectrum Trust ("OAC"), and both Chesapeake and DFW support those comments. However, Chesapeake and DFW believe that it is important to provide their own, individual support on some of the issues raised by the Commission in the *Public Notice*.

As discussed in the OAC Comments, the early builder jurisdictions have made an extensive investment in both time and capital since the issuance by the Commission of the waivers. This work has included dozens of meetings (both telephonic and in-person) with other waiver jurisdictions, the Commission, NTIA, the APCO Broadband Committee, commercial vendors, and particularly PSCR. For its part, Chesapeake has made significant contributions to the effort, both in terms of technical and governance issues. DFW has demonstrated that there are instances of extreme needs of the benefits that broadband applications can provide, and where there can be self-funding to help speed the development of the nationwide project.

As a result, the Waiver Recipients have developed a wealth of information relevant to the nationwide build-out. From technical interoperability standards to governance issues to operational issues, the work of the Waiver Recipients is an instrumental part of the ground work

[2] A copy of the application is attached hereto.

that FirstNet will be able to take advantage of when it begins operations. This work will help advance FirstNet's efforts and will help speed the development of the network.

This fact also provides the rationale for extending the Waiver Recipients' leases. Continued work and the continued implementation of systems planned, in develop and undergoing testing by Waiver Recipients will lay the foundation for completion of the network. When numerous systems are completing their plans, issuing RFPs, testing systems and preparing implementations, it makes sense to allow these early adopters to continue their work. As a result of these efforts, service can begin in many areas months, if not years, in advance of when an operational system will occur under FirstNet. The Commission (and FirstNet) should not only allow this continued work, but should encourage it to occur.

Chesapeake and DFW are sensitive to the concerns of the Commission and NTIA that the initiation of service and purchase of equipment by the early adopters may result in interoperability issues, and therefore potentially stranded investment. However, Chesapeake, DFW and other early adopters have been aware of this potential issue since the beginning. For this reason, the early adopters have been working with federal officials and system integrators to ensure, to the maximum extent possible, that the chances of lack of interoperability are minimized, and stranded investment does not happen. That has been the raison d'être of much of the work that has occurred for the last two years.

Further, Chesapeake and DFW (and it is presumed, the balance of the Waiver Recipients) have had multiple discussions with vendors and potential vendors to not only minimize the possibility of non-interoperable equipment, but to minimize the risk to the agency in the event that such non-compliance occurs. In other words, leveraging that risk to vendors has been part and parcel to the work performed by Chesapeake and DFW to date and it is believed that other

Waiver Recipients have proceeded down a similar path. As a result, the chances of potential loss to Chesapeake and/or DFW are de minimus, and far outweighed by the benefits to beginning operation as soon as possible.

Chesapeake and DFW believe that the Commission has the authority to permit extend the leases, and should do so. Extension of the leases would allow FirstNet the ability to review the situation when it is ready to begin operations, and work with Waiver Recipients to ensure a smooth transition of operations to FirstNet (should that be the methodology ultimately adopted as best for the network). The Commission (and FirstNet) should look at the work by early adopters as providing a "leg up" on construction of the network, at virtually no risk. The lessons learned from these deployments will be invaluable to FirstNet's operations.

For example, DFW's build-out will assist FirstNet in understanding how a system can be deployed in confined areas with extremely high security concerns. Because DFW has no need for outside funding for its construction, it can most easily proceed with construction, and provide a wealth of operational and other information to FirstNet. This last point is extremely important. LTE is the critical element that has been missing from the airport's police and security operations the ability to give real-time situational awareness to the officers in the airport as they respond to emergency, safety or security events on or near the airport. DFW's implementation can be perhaps the best set of "lessons" for the nationwide network. For this reason DFW, through the Texas Waiver, should be permitted to continue with its plans and begin its operations as soon as possible.

In contrast, should planned deployments be delayed (or cancelled), operational systems will not be a reality for several years. This results in a loss to safety and security in those jurisdictions, a loss of lessons learned to FirstNet, and a delay in completion of the nationwide network, requiring construction to after FirstNet has conducted all of its necessary start-up efforts, instead of having that work completed during FirstNet's initial efforts.

DFW and Chesapeake are concerned with the concept of converting the existing waivers to Special Temporary Authority (STA) licenses. The problem with this methodology is that is STA is designed for secondary, temporary authorizations, not for continuing operations. Many entities are reluctant to engage in financial arrangements when the licensee's authorization has the significant limitations attendant with any STA. While FirstNet should have the ability to review the usefulness of continued leases with the Waiver Recipients, converting the existing waivers to STAs[3] will not advance any valuable purpose.

III. CONCLUSION

WHEREFORE, the premises considered, it is respectfully requested that the Commission act in accordance with the views expressed herein.

Respectfully submitted,

CITY OF CHESAPEAKE, VIRGINIA
DALLAS-FORT WORTH
INTERNATIONAL AIRPORT

By: Alan S. Tilles, Esquire

Shulman Rogers Gandal Pordy & Ecker, P.A.
12505 Park Potomac Ave., Sixth Floor
Potomac, Maryland 20854
(301) 231-0930

Date: April 20, 2012

[3] Should FirstNet decide to continue the existing leasing arrangements, it would be more difficult for FirstNet to do so if those authorizations were STAs. Leases can be long term, STAs cannot.

SHULMAN ROGERS | GANDAL PORDY ECKER

ALAN S. TILLES | ATTORNEY
T 301.231.0930 E atilles@shulmanrogers.com

December 13, 2011

VIA ELECTRONIC MAIL

Mike Simpson
Todd Early
Mike Barney
Texas Homeland Security
Texas Department of Public Safety
5806 N. Lamar Blvd.
Austin, Texas 78752

Re: State of Texas 700 MHz Broadband Waiver
Dallas/Fort Worth International Airport User Application

Gentlemen:

This office is counsel to the Dallas/Fort Worth International Airport ("DFW"). Pursuant to the procedures established by the Federal Communications Commission ("FCC") in the grant to the Texas Department of Public Safety ("TxDPS") of a Waiver Request on May 12, 2011, the long term de facto lease between TxDPS and the Public Safety Spectrum Trust ("PSST") and the TxDPS letter of April 26, 2011 to the Region VI Public Safety Broadband Planning Council, DFW hereby submits the attached application to build a 700 MHz Broadband Public Safety System within the confines of DFW.

As discussed in the attachment, the DFW Broadband System is a fully funded project, is imperative to the safety and security of airport operations, and will be fully interoperable with all other portions of the TxDPS 700 MHz Broadband System. The DFW Broadband System is not intended as a substitute for any other network to be built by the State of Texas, but rather to serve the security needs of the DFW Airport. However, DFW Airport is aware of its obligations under the Commission's Rules to construct a system which is fully interoperable with the State of Texas and national networks. To that end, DFW fully adopts the interoperability provisions of the TxDPS letters to the FCC. Further, DFW will alter its system as necessary to comply with any revisions to that interoperability plan, including any changes subsequently made by the FCC or successor organization to the PSST.

It is respectfully requested that TxDPS act expeditiously on DFW's request. Should you have any questions, please contact me at your convenience.

Sincerely,

Alan S. Tilles, Esquire

cc: Bill Bowens, DFW Airport
Jennifer Manner, FCC
Harlin McEwen, PSST
Dusty Rhodes, DHS

DALLAS/FORT WORTH INTERNATIONAL AIRPORT

APPLICATION TO OPERATE
700 MHZ PUBLIC SAFETY BROADBAND SYSTEM

Executive Summary

Located halfway between the cities of Dallas and Fort Worth, Texas, the Dallas/Fort Worth International Airport ("DFW") is the world's third busiest, offering nearly 1,750 flights per day and serving 60 million passengers a year. DFW provides non-stop service to 144 domestic and 44 international destinations worldwide. Sitting on a campus of 18,000 acres, the airport is larger than the island of Manhattan. The Airport operates 5 passenger terminals, two full service hotels and is an international port of entry to the Unites States. For the past four years in a row, DFW has ranked in the top five for customer service among large airports worldwide in surveys conducted by Airports Council International.

DFW International Airport is an incorporated city and a sovereign jurisdiction within the State of Texas. The Airport has a commissioned police department that includes 179 sworn police officers, a fire department consisting of 195 commissioned firemen, and a private security detail of 115 security officers.

The Dallas Fort Worth International Airport is a vital part of our nation's air transportation system. The airport's mission is to provide safe and efficient passage of airline customers. In order to fulfill their mission, the airport applies resources and technologies to enhance security, improve safety and increase efficiency.

DFW maintains a Critical Communications Infrastructure to provide RF communications to all divisions of the Airport. The Airport's system was installed initially with 5-channels to support analog transmissions. The system was upgraded to 10-channels in 1995. The Radio System was upgraded to full digital ProVoice communications in November of 2001 and its communications were digitally encrypted for greater security in September of 2002.

Today, the Airport's RF communications environment consists of numerous Radio System platforms, in-building distributed antenna systems, distributed bi-directional amplifier deployments, conventional and trunked technologies. The current environment contains 800 MHz trunking, 700 MHz trunked, 450 MHz UHF conventional, 150 MHz VHF conventional, fully digital and analog transmissions capabilities and complete digital security encryption both at the radio level and the system level. The Critical Communications Infrastructure is supported by a fully fault tolerant redundant network switching center with two fully installed sites located in disparate locations. The center supports circuit switching CDMA technology from the Airport's legacy communications environment, advanced Packet switching TDMA, technology from recent system deployments, and fully compliance APCO P25 communications protocols through inner subsystem interfaced to radio systems of all major manufacturers. The Critical Communications Infrastructure is a Harris Communications Private Radio System.

DFW Airport is probably the most prominent terrorist target in the Northeastern region of the State of Texas as well as the region's largest economic generator. From a security perspective, the Airport relies heavily on technology to enables it to detect and apprehend persons that pose potential threats to the Airport. A very important need is the ability to transfer video from the Airports security surveillance environment to security officials within the passenger terminals and to police vehicles on the DFW Campus. The ability for DFW to transmit high speed data for similar reasons is also critical to the successful operations of the Airport. Decisions made regarding the use of 700 MHz broadband spectrum from the public safety trust are very important to the Airport as they affect its ability to provide a safe and secure environment for its employees, its tenants and to the traveling public.

In 2004, the airport deployed a closed circuit television (CCTC) video surveillance system. At the time, this analogue system provided unprecedented visual coverage of the Airport Operations Area (AOA). Operators viewing live video could identify risks and relay information to security personal in terminals or else ware in the AOA.

In January of 2010, the Newark Liberty International Airport experienced a security breach. An individual was able to enter through a one way door and enter the secure area without passing through screening. Without the ability to visually identify and track the individual in real time, the airport was forced to order a complete terminal evacuation. This action disrupted hundreds of flights and tens of thousands of travelers. In time, video evidence identified the individual and an arrest was made. The impact of a similar incident at DFW would be exponentially worse due to its centralized hub nature and volume of operations compared to Newark. A six hour disruption at DFW would impact thousands of flights and hundreds of thousands of travelers.

In 2010, DFW implemented a project to upgrade their CCTV surveillance system to an all I.P. digital platform. This platform would provide high definition images as well as the ability to more efficiently store, review and search for important visual information. As advanced as this new platform is, the basic communication between the video operator and the security personal responding to an incident has not changed. Video operators must relay information gathered by the surveillance system by means of voice communication. Instead of providing first responding security personal with images and live video feeds they must translate what they see into words, attempting to be both descriptive and brief.

The State of Texas LTE Network

On May 12, 2011, the Federal Communications Commission ("FCC") released an Order (*"Texas Waiver Order")* granting the State of Texas ("Texas") a conditional waiver for early deployment of a 700 MHz public safety broadband network.[1] Subsequently, the FCC approved a long term de facto lease between Texas and the Public Safety Spectrum Trust ("PSST").[2]

Pursuant to its Conditional Waiver, it is the intention of Texas to construct a statewide "system-of-regional-systems" interoperable public safety broadband network "… by way of collaboration with local/regional entities."[3] To facilitate the plan, on April 26, 2011, the Texas Department of Public Safety ("TxDPS") sent a letter to the Region VI Public Safety Broadband Planning Council (of which DFW is a member) which stated that TxDPS was "… developing a process by which TxDPS wil take applications from those entities who desire to effectively be given authority to operate in a given geographical area…"[4] On that basis, and consistent with the parameters of the TxDPS letter, the airport has determined that specific applications running over a private high speed mobile network will enhance security operations. Specifically, the airport has determined that a Long Term Evolution (LTE) network can support applications that will enable security personnel to identify and respond to security threats in a more effective and efficient manner. Therefore, DFW is presenting the following application:

[1] *See*, Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket No. 06-229, DA 11-863 (PSHSB 2011), released May 12, 2011.

[2] *See*, Public Safety and Homeland Security Bureau Approves Long Term De Facto Transfer Spectrum Lease Agreement Filed by the State of Texas to Establish a 700 MHz Interoperable Public Safety Wireless Broadband Network, PS Docket No. 06-229 (PSHSB 2011) released June 17, 2011.

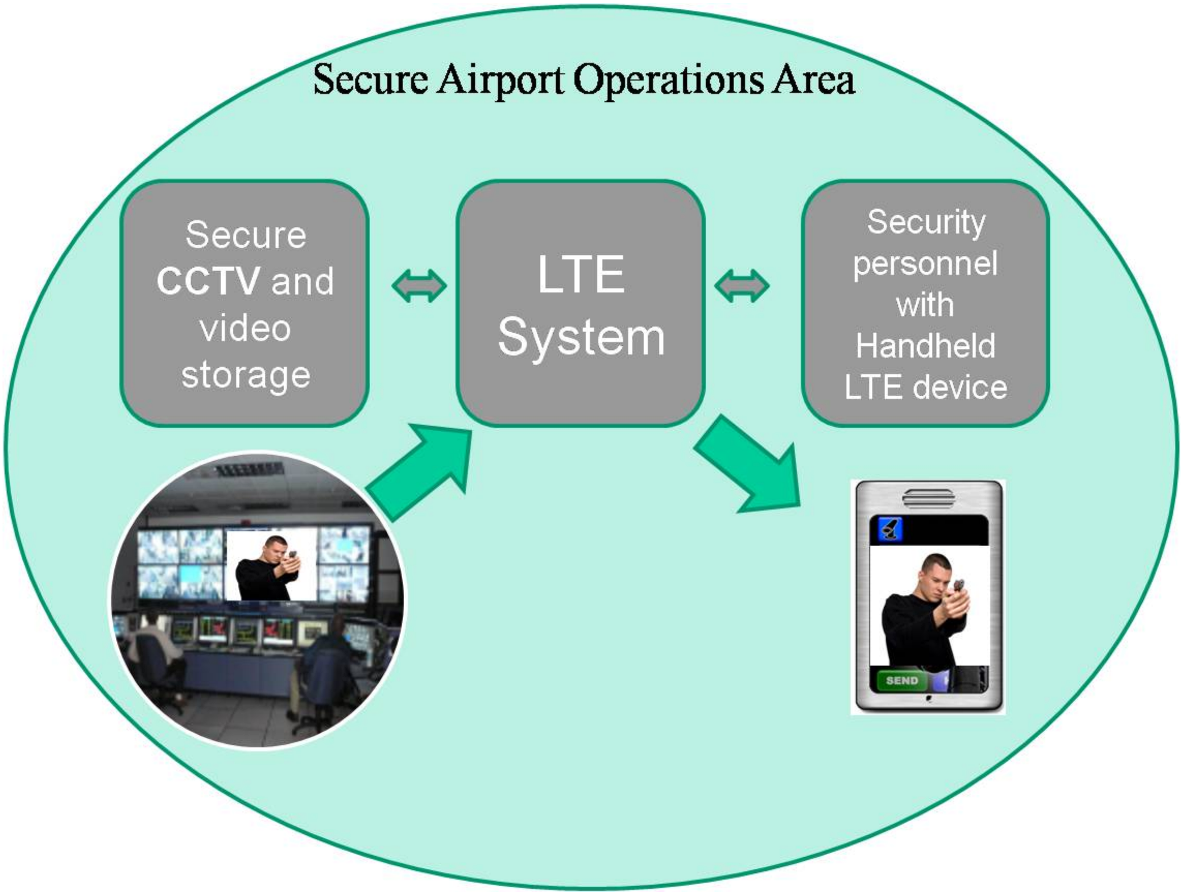
[3] *See*, Petition for Expedited Waiver, submitted by the State of Texas in PS Docket No. 06-229 on September 15, 2010 at 1-2.

[4] *See*, Attachment 1.

A Private LTE Network, Built And Operated By DFW Airport, Would Fundamentally Improve Security Operations

An LTE network would provide wireless broadband coverage across the airport property and within each terminal. This network would support a number of applications – most importantly it would provide a secure, reliable means of sharing video both from and to security personnel. Vehicles with video cameras would stream video up to the video control room where it would be viewed, archived and stored in a searchable format just as cameras currently connected to the system are.

As one example, presently the CCTV system at DFW is available only to those personnel in the dispatch center. As a result, when officers need to be dispatched throughout the terminal to find a suspect, the officers are unable to see the video feed. As a result, dispatchers most orally communicate the suspect's location and description. The implementation of the LTE network would enable the officer on the ground to "see" what the dispatcher sees on a handheld device carried by the officer, yielding higher integrity interdictions with less public disruption.


Secure Airport Operations Area
Secure CCTV and video storage
LTE System
Security personnel with Handheld LTE device
SEND

Images in the video control room could be instantly shared with security personnel responding to an incident. The ability to precisely identify and respond to security threats is absolutely essential to the airport's mission.

Because of the secure nature of all airport communications it is essential to build this network with all operating components on the airport property. The various components of the LTE network including radio base stations, serving gateways and the Evolved Packet Core (EPC) must be located and operated within the secure airport operations area. Any design that would expose the system to external security threats would not meet the airport's need. Specifically, video at the airport is governed by 49 C.F.R. §1520. This rule section provides that video such as that used at DFW (which is currently reviewed by the TSA) is Sensitive Security Information ("SSI"). Such video (including screening of goods or cargo brought into the airport) therefore may not be viewed by third parties. Therefore, DFW must have complete control over that portion of the system which provides such video capabilities.

It should be noted that the planned system will be 100% funded by the DFW Airport. Funding is already in place for the system. Thus, funding issues and delays that may be hindering other jurisdictions will not delay DFW's deployment.

DFW Broadband Plan:

DFW Airport fully supports the State of Texas objectives for a public safety broadband network. As detailed in the State's interoperability showing dated September 20, 2011:

The State of Texas recently released a clear set of high level objectives associated with the early deployment of PS LTE. Those objectives have been refined further to read:

To create an effective and interoperable 700 MHz Interoperable Mobile Public Safety Broadband Network, which, when fully deployed, will enable public safety users operating in Texas to be safer, more responsive, and more effective in the saving of lives and property.

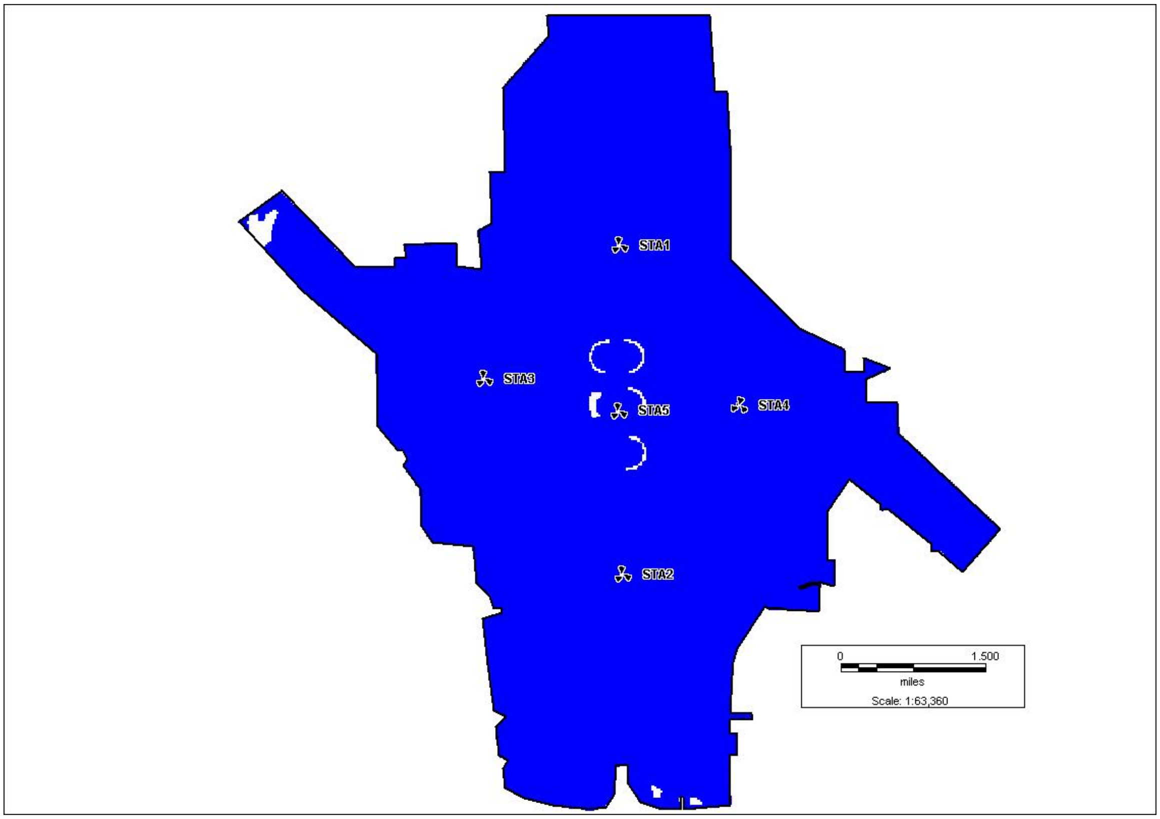
- *To enable early deployments of interoperable 700 MHz PS LTE network layers in Texas.*
- *To facilitate an open, standards-based 3rd Generation Partnership Project (3GPP) LTE environment which supports a healthy, competitive multi-vendor procurement environment for network infrastructure and terminal devices, while enabling LTE suppliers to innovate and produce sustainable products and services.*
- *To support the eventual deployment of a Nationwide Public Safety Broadband Network by working closely with agencies within Texas, other states and jurisdictions across the country, federal agency partners such as the Commission, Department of Commerce, Public Safety Communications Research program (PSCR), DHS-Office of Emergency Communications, and of course, the nationwide network governance entity (NNGE), if and when it is formed.*

- *To aggressively explore possibilities for Private/Public partnerships in order to leverage existing commercial capabilities and associated economies of scale.*
- *The network will: (1) be compliant with Release 8 of the 3GPP specification for the LTE standard; and (2) consist of an Evolved Packet Core (EPC) architecture, also known as the System Architecture Evolution (SAE), which is also a 3GPP specification for the core network. DFW will have a complete EPC, it will be a flat, all-IP core network with a simplified architecture and open interfaces. These open interfaces will enable the roaming and interoperability that are needed in a nationwide interoperable network.*

DFW plans to construct a Radio Access Network (RAN) specifically focused to provide coverage across the external Airport Operations Area (AOA) and inside the terminal areas. Although the DFW system's operational area will be confined to the airport's campus,[5] the RAN will be designed and deployed in compliance with the State's interoperability showing, Section C.1. Further, as DFW understands that the State's interoperability showing is presently under review by the FCC, DFW is aware that it may need to make changes or adjustments to its interoperability arrangements to ensure that its system is consistent with the Texas interoperability plan when it is approved. DFW will make such system changes without any request for cost reimbursement from the State or any other public safety agency or user.

> *The eNodeB (eNB) is the only 3GPP defined network element within the EUTRAN. The eNB provides the user plane and control plane protocol terminations toward the User Equipment (UE). The eNB consists of the inter-working function between the backhaul interface and the base band interface, the base band processing elements for the air interface, and the radios. The eNB in this system is compliant with the 3GPP Release 8 and Release 9 standards. The eNB is designed for compatibility with 3GPP compliant UE's and utilizes 3GPP compliant network interfaces.*

[5] This airport-restricted design also means that any regional efforts to deploy architecture on PSST spectrum will not be impacted and may proceed at whatever pace is appropriate. Further, because the system is confined to the airport, there has been no need for the regional open meetings discussed in the April 26, 2011 TxDPS letter. Rather, DFW has obtained the "buy-in from the many public safety agencies to be covered by the planned LTE layer." That group consists of DFW, TSA and DHS employees. However, it should be noted that DFW Airport will work with any regional effort to ensure maximum interoperability pursuant to adopted rules.

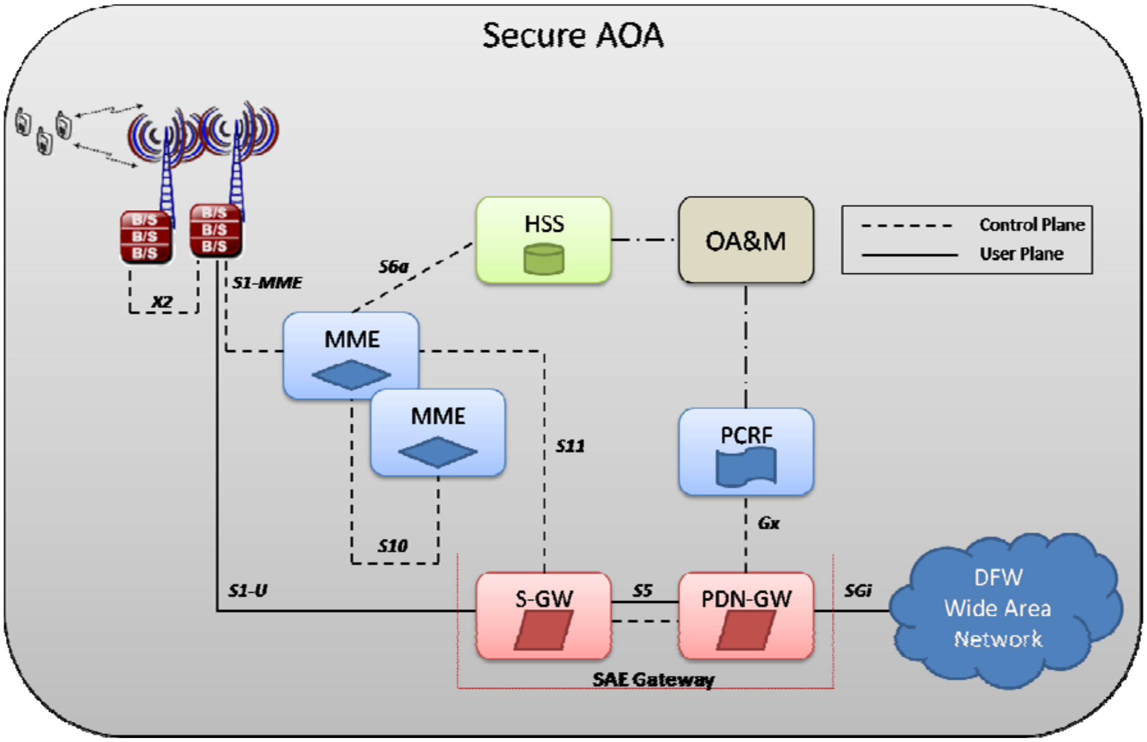


Planned coverage of DFW Airport

Core Network Architecture

The core network will be designed and deployed in compliance with the State's interoperability showing, Section C.2

> *The core network is based on the 3GPP R8 defined EPC as mainly defined in 3GPP TS 23.401. The solution will support the MME, SGW, PGW, HSS and PCRF functions using standards defined network interfaces. A VPN element is also shown. This element supports a secure public safety VPN and can be used with alternate access technologies (e.g., WiFi and 3G)….*



The various components of the LTE network including radio base stations, serving gateways and the Evolved Packet Core (EPC) must be located and operated within the secure Airport Operations Area (AOA). As discussed previously, the FAA and TSA mandated security requirements at the airport mean that any design that would expose the system to external security threats would not meet the airport's need.

Interfaces

The system will contain and use the following interfaces that are in compliance with the State's interoperability showing, Section C.3:

- *Uu – LTE over the air interface*
- *S1-MME – eNb and the MME*
- *S1-u – eNb and the SGW*
- *S5 – SGW and PGW*
- *S6a – Visited MME and the Home HSS*
- *S8 – Visited SGW and Home PGW*
- *S9 – Visited PCRF and Home PCRF*
- *S10 – MME to MME for Category 1 Handover*
- *S11 – MME and SGW*
- *SGi – PGW and external PDN*
- *X2 – eNodeB to eNodeB*
- *Gx – PGW and PCRF*
- *Rx – PCRF and AF located in PDN*
- *Gy/Gz – online/offline charging interfaces*

> *These interfaces support interoperability of the LTE network with 3GPP R8 December 2009 freeze or R9 September 2010 freeze compliance. These standards apply to UE devices, as well as interoperability with other PS regional LTE networks. Details on handoff and mobility inter-operability are addressed in Section C.4 including mobility across regional PS LTE networks.*

Mobility and Handoff

The system will be designed and deployed in compliance with the State's interoperability showing, Section C.4

> *The State of Texas commits to supporting mobility and handover, such that users have a smooth and seamless transition between eNode sites wherever possible. The handover functionality can be supported using one of the many options available in the LTE architecture…*

Roaming

The system will be designed and deployed in compliance with the State's interoperability showing, Section C.5

> *Roaming is the ability for a user to obtain service in a visited network. Roaming will be supported with other regional networks across the nationwide Shared Wireless Broadband Network (SWBN). These requirements are supported by leveraging 3GPP standardized interfaces, as well as adoption of a roaming services tailored to the SWBN.*

As discussed above, DFW is a participant in the Region VI Network Architecture Working group and supports the multi-vendor architecture goals of this working group. DFW is committed to integrate the e DFW core into this multivendor interoperability architecture. Until this architecture framework is resolved, the DFW system will be able to use the Intra-system roaming as defined in Section C.5.2 to interoperate between users from the Harris County core and DFW core (or any other core installed using PSST spectrum). DFW will support IMSI partitioning and Intra-system roaming as defined for the National broadband network.

The proposed DFW system deployment will implement a network identifier schema in accordance with the plan adopted by the State in conjunction with the PSCR Network Identifier Study Item Group. The State and PSCR intend to define a network identifier schema that will allow the allocation of global identifiers for current deployments that will assure integration into a national network at a later date. In the case of a single PLMN ID, the schema will include an IMSI partitioning plan in support of an Intra-system roaming architecture. DFW is aware that this architecture will most likely require the deployment of a DIAMETER Routing Agent.[6]

It should be noted, however, that initial deployment of this system is designed for DFW high security operations. Thus, there will not be an initial need for DFW deployed units to have interoperability with any other PSST spectrum system.[7] Therefore, the DFW system can be deployed, prior to finalization of network rules, with no impact to users, should the final network rules differ significantly from what is currently contemplated.

Priority Access and QoS

The system will be designed and deployed in compliance with the State's interoperability showing, Section C.6

> *LTE offers the most advanced QoS capabilities of any commercial cellular technology; however the technology must be properly configured for optimal public safety implementation. The State of Texas is working with the public safety and vendor communities to contribute to the development of interoperable priority access and QoS requirements. The implementation will be compliant with 3GPP TS 23.203. All of the (QoS Class Identifier) QCI (1-9) and (Allocation and Retention Parameters) ARP (1-15) values defined in this specification will be supported in the deployed equipment. In addition, all of the Access Class (0-15) values as defined in TS 22.011 will be supported.*

Security

The system will be designed and deployed in compliance with the State's interoperability showing, Section C.7

> *Security is a critical aspect of the public safety broadband network implementation. Therefore, the State of Texas commits to supporting the optional security features specified in 3GPP TS 33.401, which include integrity protection, verification of data and ciphering and deciphering of data. The State also commits to supporting network layer VPNs.*

[6] It should be noted that the exact rules for the PSST's network are still being developed by the PSST, the FCC and various other entities. DFW affirmatively states that it will adhere to the final rules developed for this spectrum. This recognition includes DFW's acknowledgement that DFW may be required to reprogram subscriber units deployed prior to finalization of network rules or even to discontinue use of the DFW core as a primary core.

[7] Further, because of TSA security policies, other PSST spectrum users "roaming" into DFW will not be able to access these high security portions of the DFW system.

Overall Security Architecture

The system will be designed and deployed in compliance with the State's interoperability showing, Section C.8

3GPP standards have defined a suite of security related specifications for LTE systems. The 33 series of 3GPP specifications contains several documents defining various aspects of LTE and broadband application security architectures. From an interoperability perspective, of particular interest are the specifications 33.401 ("3GPP System Architecture Evolution (SAE); Security architecture"), 33.210 ("3G security; Network Domain Security (NDS); IP network layer security"), and 33.310 ("Network Domain Security/Authentication Framework (NDS/AF)"). The implementation will fully support the requirements stated in these specifications to ensure secure inter-system interoperability. The implementation will support both the mandatory and optional aspects of the 3GPP SAE security architecture specification, as defined in 33.401.The optional aspects align with recommendations given by the NPSTC Broadband Task Force.

Network Domain Security

The system will be designed and deployed in compliance with the State's interoperability showing, Section C.9

The implementation will utilize the 3GPP defined mechanisms for Network Domain Security, as defined in the 3GPP spec 33.210, "Network Domain Security, IP Network Layer Security". Per 33.210, the interfaces between the network entities in the network are to be secured using IPsec security associations. The security associations will be established and maintained using either IKE (Internet Key Exchange) v1 or IKEv2. Per 33.210, the Za interface is used to interface between two security domains and the Zb interface is used to interface between the various network entities within a single security domain. Specifically:

- *NDS/IP inter-domain interface (Za) cryptographic protection via Security Gateways (SEGs) will be provided. The Za interface security associations will be established using IKEv1 or IKEv2. X.509 digital certificate based authentication will be utilized between SEGs in different security domains.*

- *NDS/IP intra-domain interfaces (Zb) as specified in 33.210 will be cryptographically protected unless within physically secure and/or fully trusted environments.*

MVPN Access to Home

The system will be designed and deployed in compliance with the State's interoperability showing, Section C.10

> *The Waiver Order requires petitioners' systems allow the use of network layer VPN access to any authorized site and to home networks on the deployed network. This requirement is designed to ensure the ability of first responders to securely connect back to their home systems when attaching to foreign wireless networks. Without this requirement, there is the risk some deployments may have their wireless networks configured to discard any traffic that is encrypted and destined to an external domain. This would be very problematic, as there are security compliance policies by CJIS, and NCIC (National Crime Information Center) that require the use of VPNs for remote user access.*
>
> *CJIS (Criminal Justice Information System) requirements mandate the use of FIPS 140-2 validated encryption. Thus any user of a deployment utilizing a broadband waiver must use*
> *FIPS 140 validated implementations to be compliant with CJIS security policy and to access CJIS related services. The implementation will use FIPS 140-2 compliant VPN solutions for remote user access.*

Devices

DFW will deploy devices in compliance with the State's interoperability showing, Section C.11

> *Delivery of user devices for Public Safety broadband agencies will be driven by the availability of LTE chipsets supporting standard 3GPP baseband protocols and RF operation in the 10 MHz of Public Safety spectrum (763 MHz to 768 MHz lower and 793MHz to 798 MHz upper). All devices will adhere to the 3GPP Release 8 or later air interface specification and the recommended out of band emissions (OOBE) as specified in the Waiver Order, as well as existing OOBE requirements to protect Public Safety narrowband voice services in the 700MHzspectrum.*

Conclusion:

DFW desires to deploy a sustainable state of the art broadband network using standards compliant 3GPP LTE technology. DFW is cognizant of the amount of planning and consideration required to successfully deploy a network of this type, particularly the need to integrate the network as part of a larger state-wide and nationwide network. While the system is designed primarily to serve the internal public safety needs of DFW Airport, the system will be constructed to enable full interoperability with the national public safety LTE network. To this end, it is the intention of DFW to fully comply with the recommendations and requirements as defined by the State of Texas, the PSRC Demonstration Network, and the FCC.